# Deep learning for Android forensic analysis: a multimodal approach.

Okangondo Loshima Junior*, Serigne Modou Kara Samb**, Mohamed Kaba Keita***, Omatete Okitodinga Jacques****,
Moussa Dethie Sarr**, Idy Diop***
*Faculty of Science and Technology, University Cheikh Anta Diop of Dakar, Dakar 630-0101, Senegal
**Science technology mathematics computer science, iba der thiam university, thies, Senegal
***Ecole Supérieure Polytechnique, University Cheikh Anta Diop of Dakar, Dakar 630-0101, Senegal
**** Faculty of Science and Technology, University Patrice Emery Lumumba University of Wembo-Nyama, Sankuru,
Congo RD.
juniorokangondoloshima@esp.sn, smkara.samb@univ-thies.sn, keita.mohamed@esp.sn, omatetejacques@gmail.com,
mdsarr@univ-thies.sn, idy.diop@esp.sn

***Abstract* — We present a multimodal forensic framework optimized for detecting malicious activity on Android, integrating static, dynamic, and network artifacts. Our architecture combines CNN, LSTM, and Autoencoders within a hybrid fusion: early and late, allowing us to capture both inter-modal correlations and the specificities of each type of data. Embedded optimizations, such as pruning, quantization, transfer learning, and incremental learning, ensure efficient deployment on constrained Android devices while maintaining accuracy. The data we used in this study comes from public datasets, Drebin and CIC-AndMal2017, and from controlled captures, with pre-processing to ensure normalization, temporal alignment, and preservation of probative value. The evaluation was conducted both in a controlled environment and in real-world conditions on Android 13 smartphones. Our results show that hybrid fusion outperforms single-model approaches, achieving 94.8% accuracy, 94.0% F1 score, and a false positive rate limited to 3.8% in real-world conditions, with an average latency of 20 ms, thus ensuring near real-time detection. This performance is maintained despite the variability of network flows and application behaviors observed in the field. In addition to robustness and computational efficiency, our approach enhances interpretability through the integration of explanatory tools such as SHAP and LIME, which meet medico-legal requirements for transparency and reliability of digital evidence. Our outlook is focused on adaptive, scalable, and large-scale deployable detection systems.***

**Keywords — Android forensics, anomaly detection, deep learning, mobile malware.**

Junior O. Loshima was born in the Democratic Republic of Congo. He received the Master’s degree in software engineering from the Université Numérique Cheikh Hamidou Kane, Dakar, Senegal, in 2021, and the Master’s degree in cybersecurity from the École Supérieure Polytechnique, Dakar, Senegal, in 2022. He is currently pursuing the Ph.D. degree in computer science at the École Doctorale de Mathématiques et Informatique of the Université Cheikh Anta Diop, Dakar, Senegal, where his major field of study focuses on digital forensics and the development of investigation systems tailored for low-resource environments.

He has been a Mentor in Software Development and Cybersecurity at FORCE-N, Dakar, Senegal, since 2023, where he designs training programs, supervises cybersecurity projects, and develops secure applications for educational and operational environments. He also serves as a Lecturer in cybersecurity and digital forensics at the École Supérieure Polytechnique, Dakar, where he teaches data confidentiality, digital investigations, and practical laboratory techniques for post-mortem analysis and cyberattack investigation. His work includes the development of digital forensics platforms used for academic training and research, as well as contributions to the study of forensic infrastructures for developing countries. His research interests include digital forensics, cybersecurity of emerging technologies, machine learning–based anomaly detection, secure software engineering, and cyber-crime analysis.

Mr. O. Loshima is certified in Ethical Hacking Essentials, SQL Injection Attacks (EC-Council), MCSE Server Infrastructure, ITIL, CompTIA Security, and ISO 27001. He is the author of ongoing research on forensic optimization in low-resource infrastructures and Android log-based anomaly detection. He has contributed to academic and professional training programs in cybersecurity and has participated in the development of forensic methodologies adapted to African contexts.